REMARKS

The Examiner has rejected Claims 1-10, 12-30 and 32-39 under 35 U.S.C. 102(e) as being anticipated by Maloney et al. (U.S. Pat. No.: 6,549,208). Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1, 24, 28 and 36 (containing the same or substantially similar, but not identical, claim language), the Examiner has relied on the following excerpt from Maloney to meet applicant's claimed "prior to the certain electronic file being made available for viewing by the intended recipient, converting the certain electronic file to a second file format that is different from the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient."

> "Data in the knowledge base 16 is made available to a data parsing tool 18 that converts the captured network data from the discovery tool 12 to a form useable by downstream programs of the system. Data accessed by the parsing tool 18 is then available to analytical engine 20 for analyzing the data captured by the discovery tool 12 and supports the merging of several data files and the development and comparison of network usage patterns." (see col. 4, lines 39-42 - emphasis added)
>
> "The query consult tool 94 provides a text-based interface to the knowledge base 16. By utilization of the query consult tool 94, a user is able to determine if the knowledge base 16 contains an object (for example, individual IP address) or determine the set of objects belonging to a class of the knowledge base 16 (for example, IP-ADDR). In one implementation of the query consult tool 94, the knowledge base 16 was queried for top level class names, objects belonging to a given class and specific class objects." (Col. 9, lines 45-53 - emphasis added)

Applicant respectfully disagrees with this assertion. In particular, Maloney simply discloses that "[d]ata in the knowledge base 16 is made available to a data parsing tool 18 that converts the captured network data from the discovery tool to a form usable by downstream programs..." (see emphasized portion of relevant excerpt above). In addition, it is noted that "the discovery tool 12 collects **traffic and usage data** and maps the network connectivity" (see Col. 4, lines 28-29 - emphasis added). Examples of such collected data is also disclosed in

Maloney, including, "Address, Host, LM-Host, Domain, LM-Domain, SubNet, IP-Address..." (see Col. 4, lines 32-38).

Therefore, Maloney teaches converting captured network data that includes traffic and usage data in order for the data to be usable by other downstream programs, and not "converting the certain electronic file to a second format that is different from the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient," as claimed by applicant. Furthermore, Maloney's teaching of querying for class object and classes (as cited above) does not in any way relate to converting that prevents the computer virus from executing, as claimed by applicant. Simply nowhere in Maloney is there any suggestion of converting a file format to "[prevent] the computer virus from executing when the converted electronic file is opened by the intended recipient."

In addition, the Examiner has relied on the following excerpts from Maloney to meet applicant's claimed "said converting the certain electronic file being in response to a determination that the certain electronic file represents the potential risk to the security of the computer system."

> "...locate the existence of backdoors, reduce bandwidth usage, develop profiles of users, and pinpoint illicit activity." (Col. 2, lines 2-3)
>
> "...determination of potential choke points and vulnerabilities..." (Col. 6, line 33)
>
> "Following parsing of the **knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams.** Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate." (Col. 6, line 66-Col. 7, line 4 - emphasis added)

Applicant respectfully asserts that Maloney's teaching of converting the knowledge base data into vector-based nodal diagrams in no way relates to "converting the certain electronic file in response to a determination that the certain electronic file represents the potential risk to the security of the computer system," as claimed by applicant. Specifically, Maloney's converting relates to converting traffic and network usage data into a usable form for other programs, as cited above, and not to converting electronic files in response to potential security risks. Therefore, Maloney fails to even suggest "converting an electronic file in response to a

determination that the certain electronic file represents the potential risk to the security of the computer system" (emphasis added), as claimed.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Maloney reference, for the reasons noted above. In addition, applicant respectfully asserts that the Maloney reference is further deficient with respect to the dependent claims.

With respect to dependent Claim 4 et al., the Examiner has relied on Maloney's disclosure of utilization of a PC in implementing the information security analysis system (Col. 5, lines 59-61) to make a prior art showing of applicant's claimed "receiving occurring at a desktop computer of the intended recipient." Applicant respectfully asserts that Maloney's general utilization of a PC does rise to the specificity of applicant's claim language wherein the electronic file, as recited in each of the independent claims, is received at a desktop.

With respect to dependent Claim 5 et al., the Examiner has relied on Maloney's mention of an HTTP-Server to make a prior art showing of applicant's claimed, "said receiving occurring at a server computer." It seems the Examiner has failed to take Maloney's mention of an HTTP-Server in context. Applicant notes that, in the proper context of Maloney's disclosure, data about HTTP-Servers is collected and becomes part of the knowledge base. Therefore, there is no receiving [of an electronic file] occurring at a server computer," as claimed by applicant.

With respect to dependent Claims 7-8 et al., the Examiner has relied on the following excerpts et al. from Maloney to make a prior art showing of applicant's claimed "said converting at a desktop computer of the intended recipient"(Claim 7) and "said converting occurring at a server computer"(Claim 8).

"The hardware platforms consist of several different types of interconnected computers..."(Col. 2, lines 24-25)

"...HTTP-Server..."(Col. 4, line 36)

"An internal packet processing engine 36 decodes data packets and converts the raw data to information elements that are accessible to all the tools in a tool suite 34."(Col. 7, lines 30-33)

Applicant respectfully points out that the above excerpts from Maloney merely mention an HTTP-Server and interconnected computers and that when taken in context, as describe above with regard to Claim 5, do not disclose "converting [the electronic file] at a desktop computer of the intended recipient" nor "converting [the electronic file] at a server computer," as claimed by applicant. To emphasize, there is simply no suggestion in Maloney of converting an electronic file format at a desktop computer or server.

With respect to dependent Claim 10 et al., the Examiner has relied on Maloney's mere mention of determining whether a computer virus is present prior to its execution on the host computer to meet applicant's claimed "said converting occurring prior to the intended recipient receiving the certain electronic file." Applicant emphasizes that Maloney *teaches away* from applicant's claim language by determining whether a computer virus is present prior to its execution on the host computer, whereas applicant claims "converting [the electronic file] occurring prior to the intended recipient receiving the certain electronic file" (emphasis added).

In addition, Maloney simply teaches determining whether a virus is present while applicant claims "converting prior to the intended recipient receiving the certain electronic file." Thus, Maloney is clearly deficient with respect to the limitations of Claim 10 et al.

With respect to dependent Claim 13, the Examiner has relied on the following excerpt in Maloney to make a prior art showing of applicant's claimed "said determining whether the certain electronic file represents the potential risk comprising: conducting a heuristic scan of the certain electronic file."

"...provided viewing of the following sessions: HTTP, POP3, TELNET, FTP, SMTP, NNTP, and IMAP. During operation of the session recorder tool 92 data can be added to the knowledge base 16 as the tool detects,

processes and scans sessions for various pieces of information." (Col. 9, lines 39-44)

Applicant respectfully asserts that the above excerpt fails to even suggest "conducting a heuristic scan of the certain electronic file," as claimed by applicant. Maloney merely discloses detecting, processing and scanning sessions (HTTP, POP3, etc) for various pieces of information. This simply does not rise to the level of specificity of applicant's claim language wherein "a heuristic scan of the certain electronic file" (emphasis added) is conducted to determine "whether the certain electronic file represents the potential risk."

With respect to dependent Claim 14, the Examiner relies on the following excerpts from Maloney to make a prior art showing of applicant's claimed "receiving a second electronic file intended for delivery from another sender to another intended recipient, the second electronic file having a third file format and containing another computer virus; and prior to the second electronic file being made available for viewing by the another intended recipient, converting the second electronic file to a fourth file format that is different from the third file format and that prevents the another computer virus from executing when the second electronic file is opened by the another intended recipient."

"A second analytical engine from the Department of Defense..."(Col. 4, line 49)

"The addition of a third vector permits the simultaneous viewing of large complex diagrams on interconnected planes in accordance with user instructions from the input device 94. The display of FIG. 5 permits an analyst to rotate the diagram on any axis thereby viewing relationships that otherwise become obscure viewed on two-dimensional planes." (Col. 11, lines 36-41)

"In this example the analysis system 10 as running on the terminal 70 monitors the level of intranet traffic and records packets of data from each of the terminals of the various nodes. For a terminal under attack, such as terminal 64a, the analysis system establishes a target source packet structure and by means of the analytical engine 20 of the present invention could be modified to shut down a target under attack." (Col. 12, lines 15-24)

Applicant respectfully asserts that Maloney's teachings of "a second analytical engine", "simultaneous viewing of large complex diagrams" and "monitor[ing] the level of intranet traffic...from each of the terminals of the various nodes" fail to meet applicant's claim limitations. Specifically, neither the above excerpts nor the entire Maloney reference, disclose

"receiving a second electronic file intended for delivery from another sender to another intended recipient... containing another computer virus... converting the second electronic file... that prevents the another computer virus from executing..." (emphasis added), as claimed by applicant.

With respect to dependent Claim 16 et al., the Examiner has relied on the following excerpt from Maloney to make a prior art showing of applicant's claimed "the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format."

> "...parsing and formatting of data from HTML flat files that are then imported to a database or to the analytical engines." (Col. 10, lines 24-25)

Applicant respectfully points out that the above excerpt from Maloney does not teach a second file format (wherein the electronic file was converted from a first file format to a second file format in the context of Claim 1), let alone a second file format that includes one of the formats enumerated above in claim 16 et al. Maloney simply teaches formatting data from HTML and importing the data into a database, and thus fails to meet applicant's claim limitations.

With respect to dependent Claims 17-18, the Examiner has relied on the same excerpt as with Claim 16 in rejecting applicant's claimed "the second file format being the HTML file format without scripts" (see Claim 17) and "the second file format being the TXT file format" (see Claim 18). Again, applicant respectfully asserts that Maloney teaches formatting data from HTML to a database, whereas applicant claims the second file format (formatted from a first file format in the context of Claim 1) being the HTML file format without scripts (Claim 17) and the TXT file format (Claim 18).

With respect to dependent Claim 21, the Examiner has relied on the following excerpts from Maloney to make a prior art showing of applicant's claimed "the certain electronic file being at least one of a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file."

"This text knowledge base flat file is processed by the data parsing tool 18..." (Col. 6, lines 55-56)

"The graphics extraction tool of the knowledge base toll set 96 provides for reassembling image files forma recorded format." (Col. 10, lines 30-33)

Applicant respectfully asserts that the above excerpts from Maloney do not teach or even suggest the "certain electronic file being at least one of a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file," as claimed by applicant. The above excerpts from Maloney even fail to make any mention of an electronic file, as claimed by applicant in the context of Claim 1.

With respect to dependent Claim 22 et al., the Examiner relies Maloney's disclosure of a graphics extraction tool providing for reassembling image files (Col. 10, lines 30-32) to make a prior art showing of applicant's claimed "determining if the first file format is one of a word processing file format type and a graphics file format type." Clearly this disclosure from Maloney in no way even suggests "determining if the first file format is one of a word processing file format type and a graphics file format type" (emphasis added), as claimed by applicant since it simply discloses utilization of a graphics extraction tool to reassemble image files.

In addition, the Examiner relies on Maloney's disclosure of processing the format of a flat text file from the discovery engine (Col. 6, lines 52-53) to make a prior art showing of applicant's claimed "the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the certain file format is the word processing file format type." Maloney's mere disclosure of processing the format of a text file completely fails to make any suggestion of determining whether "the certain file format is the word processing file format type" and then converting the first file format type (in the context of Claim 1) to be "at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the certain file format is the word processing file format type".

Further, the Examiner again has relied on Maloney's disclosure of a graphics extraction tool providing for reassembling image files (Col. 10, lines 30-33) to make a prior art showing of

applicant's claimed. "the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type." Again, applicant respectfully asserts that Maloney's mere mention of image files completely fails to make any suggestion of determining whether "the certain file format is the graphics file format type" and then converting the first file format type (in the context of Claim 1) to be "at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type."

With respect to dependent Claim 25, the Examiner has relied on the following excerpt from Maloney to make a prior art showing of applicant's claimed "said determining comprising: determining whether the electronic file has a file extension indicative of a file type that supports a potential computer virus."

> "Data accessed by the parsing tool 18 is then available to analytical engine 20 for analyzing the data captured by the discovery tool 12 and supports the merging of several data files and the development and comparison of network usage patterns. The analytical engine 20 may be implemented by software from i2 Inc. and marketed under the trademark "Analyst's Notebook". A second analytical engine 20 from the Department of Defense called PROPELLER is also available. The present invention is also capable of utilizing additional analytical engines as such engines become available. The analytical engines 20 are a dynamic set of graphic tools for capturing and displaying a variety of relational data sets in a format referred to as a "link chart". By use of the analytical engine 20, such as "Analyst's Notebook", data collected can be exploited to characterize and document network characteristics and/or locate possible network intruders. After collecting and organizing data, the analytical engine 20 can be used to make associations between a number of different data charts to determine correlation or differentiation." (Col. 4, lines 42-61)

Applicant respectfully asserts that the above excerpt from Maloney does not even suggest "determining whether the electronic file has a file extension indicative of a file type that supports a potential computer virus" (emphasis added), as claimed by applicant. Maloney, as cited above, simply locates possible network intruders according to data collected, but fails to suggest that such collected data includes a file extension indicative of a file type that supports a potential computer virus.

With respect to dependent Claim 27, the Examiner has relied on Maloney's disclosure of examining the functionality of suspect code to determine if a compute virus is present prior to its execution in the host computer (see Col. 2, lines 48-51) to make a prior arts showing of applicant's claimed "said determining comprising: determining whether the content of the electronic file reflects a potential computer virus." Applicant specifically points out that Maloney determines if in fact there is a computer virus according to the functionality of suspect code whereas applicant claims "determining whether the content of the electronic file reflects a potential computer virus."

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P092/01.050.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100